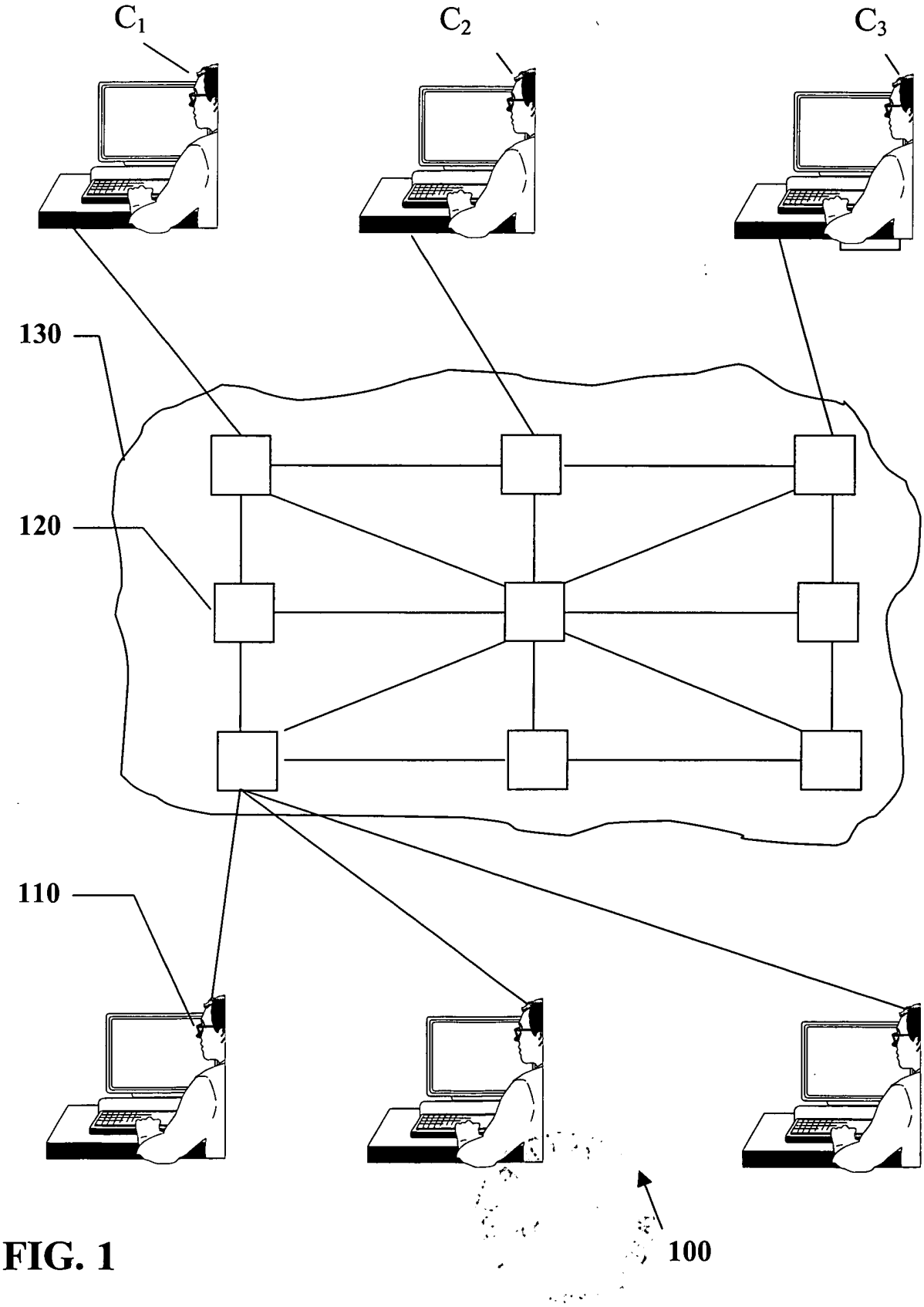

FIG. 1

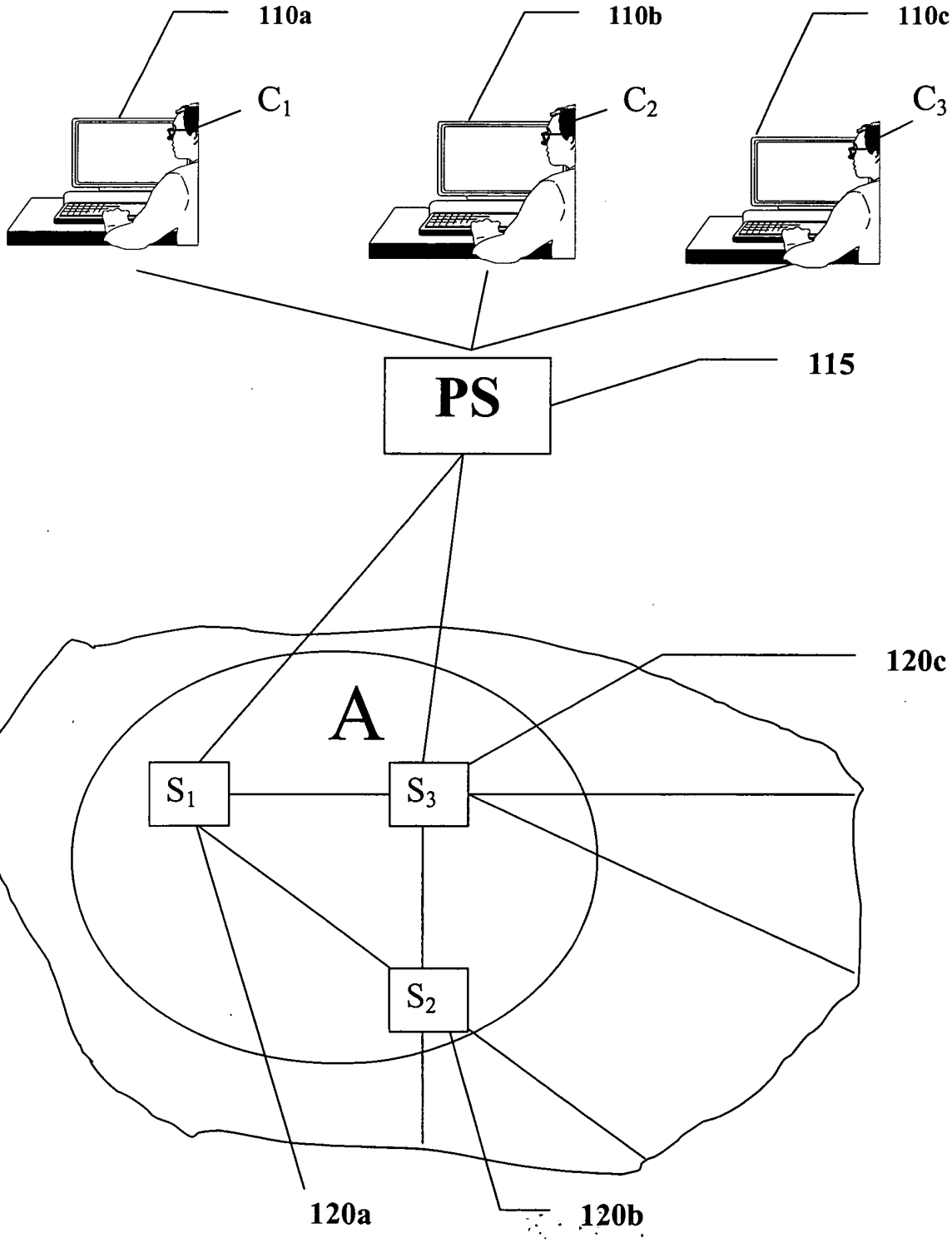

FIG. 2

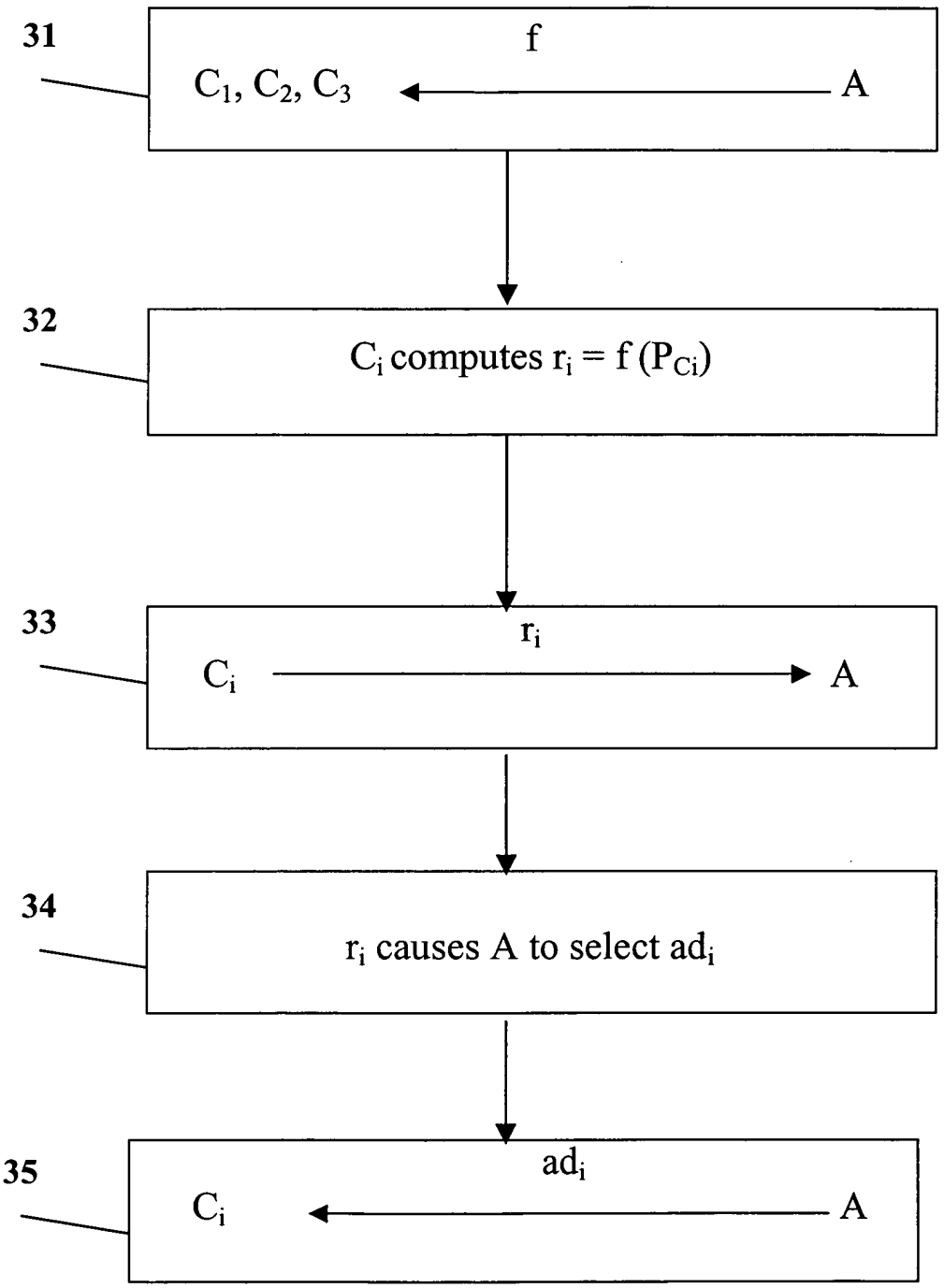
31
f
C_1, C_2, C_3
A
32
C_i computes $r_i = f(P_{Ci})$
33
r_i
C_i
A
34
r_i causes A to select ad_i
35
ad_i
C_i
A

FIG. 3

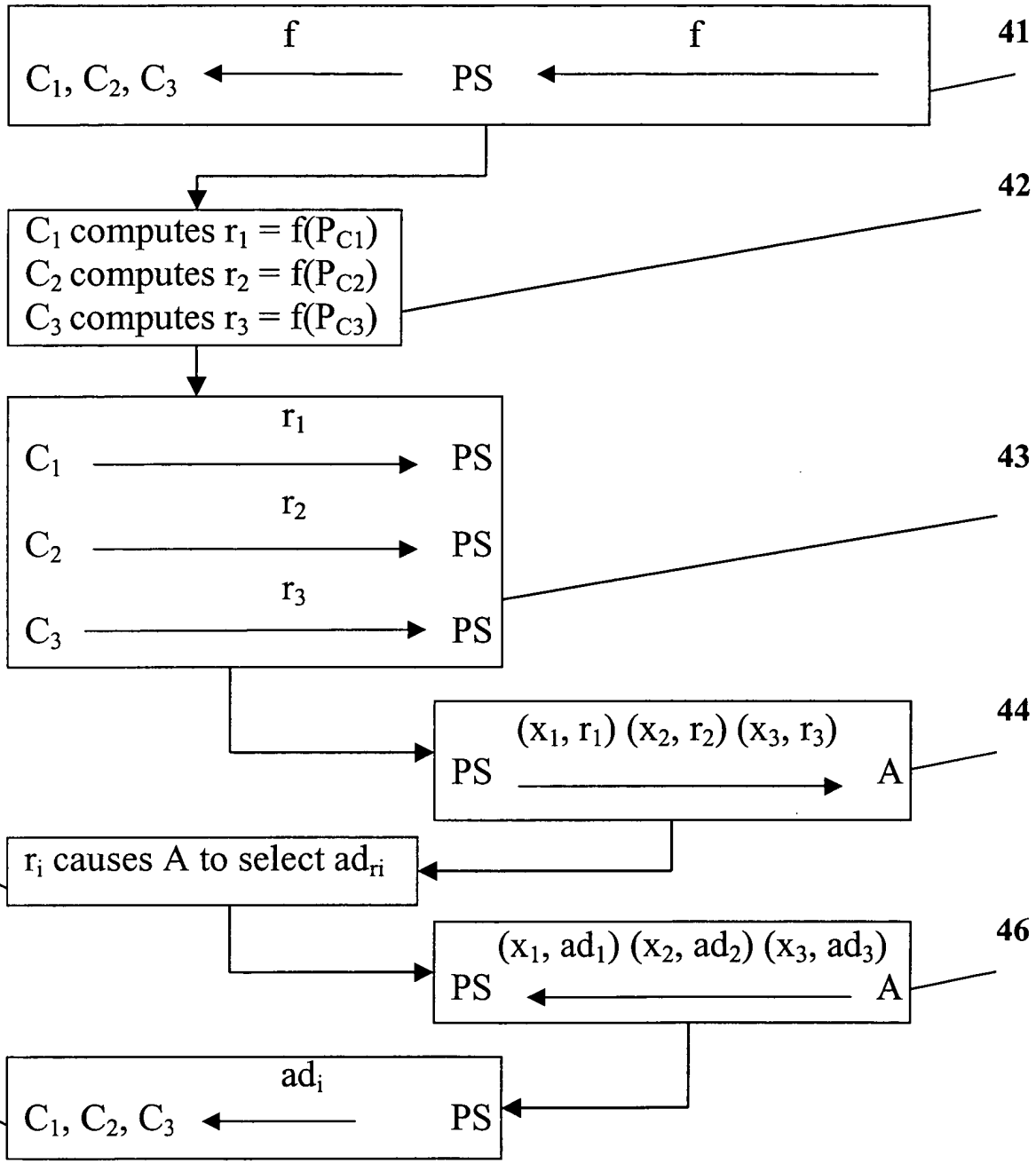
f
f
C_1, C_2, C_3
PS
41
C_1 computes $r_1 = f(P_{C1})$
C_2 computes $r_2 = f(P_{C2})$
C_3 computes $r_3 = f(P_{C3})$
42
r_1
C_1
PS
r_2
C_2
PS
r_3
C_3
PS
43
(x_1, r_1) (x_2, r_2) (x_3, r_3)
PS
A
44
45
r_i causes A to select ad_{ri}
(x_1, ad_1) (x_2, ad_2) (x_3, ad_3)
PS
A
46
47
ad_i
C_1, C_2, C_3
PS

FIG. 4

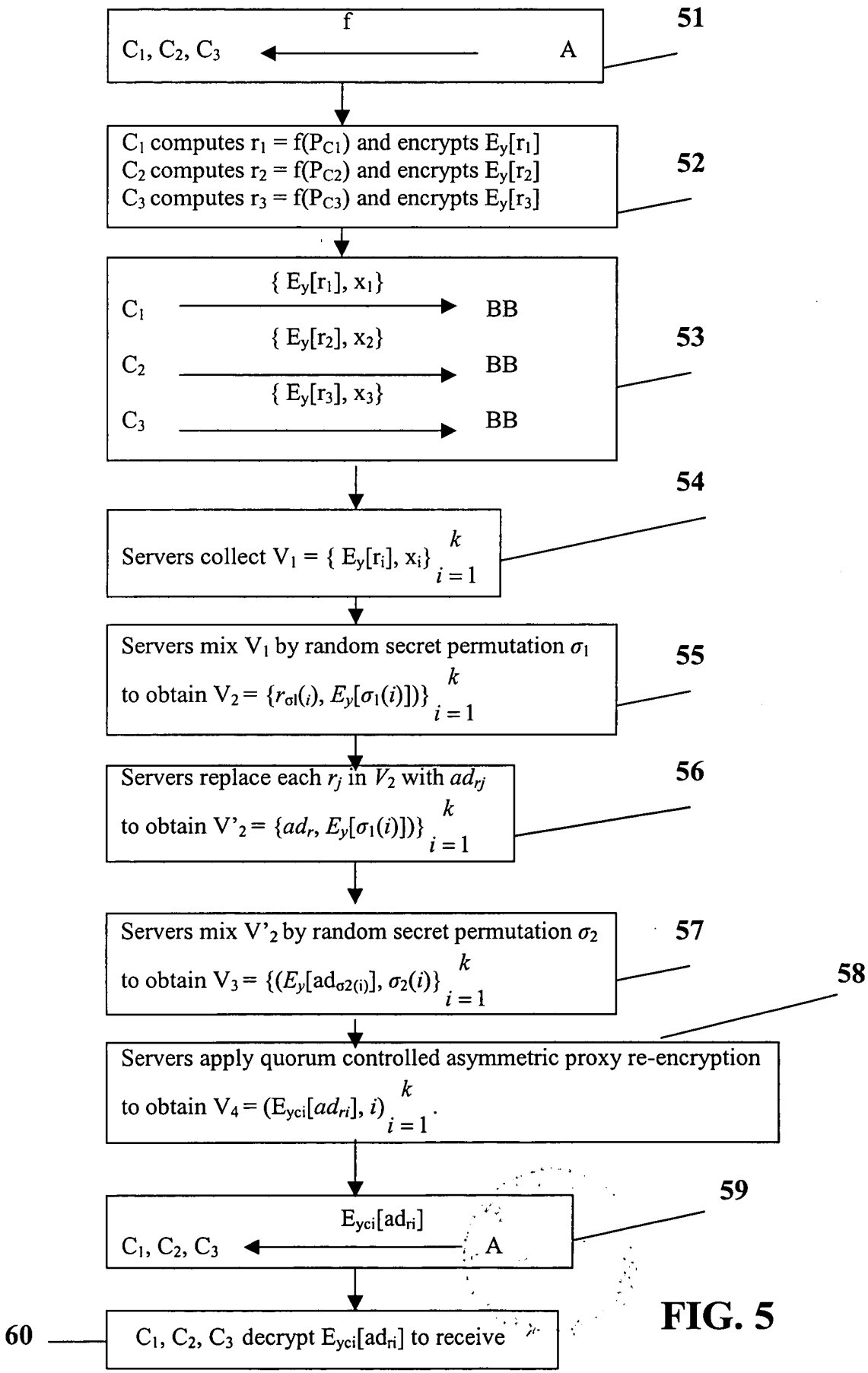
51
f
C1, C2, C3
A
52
C1 computes r1 = f(PC1) and encrypts Ey[r1]
C2 computes r2 = f(PC2) and encrypts Ey[r2]
C3 computes r3 = f(PC3) and encrypts Ey[r3]
53
{ Ey[r1], x1}
C1
BB
{ Ey[r2], x2}
C2
BB
{ Ey[r3], x3}
C3
BB
54
Servers collect V1 = { Ey[ri], xi} k i=1
55
Servers mix V1 by random secret permutation σ1
to obtain V2 = {rσ1(i), Ey[σ1(i)]} k i=1
56
Servers replace each rj in V2 with adrj
to obtain V'2 = {adr, Ey[σ1(i)]} k i=1
57
Servers mix V'2 by random secret permutation σ2
to obtain V3 = {(Ey[adσ2(i)], σ2(i)} k i=1
58
Servers apply quorum controlled asymmetric proxy re-encryption
to obtain V4 = (Eyci[adri], i) k i=1
59
Eyci[adri]
C1, C2, C3
A
60
C1, C2, C3 decrypt Eyci[adri] to receive

FIG. 5

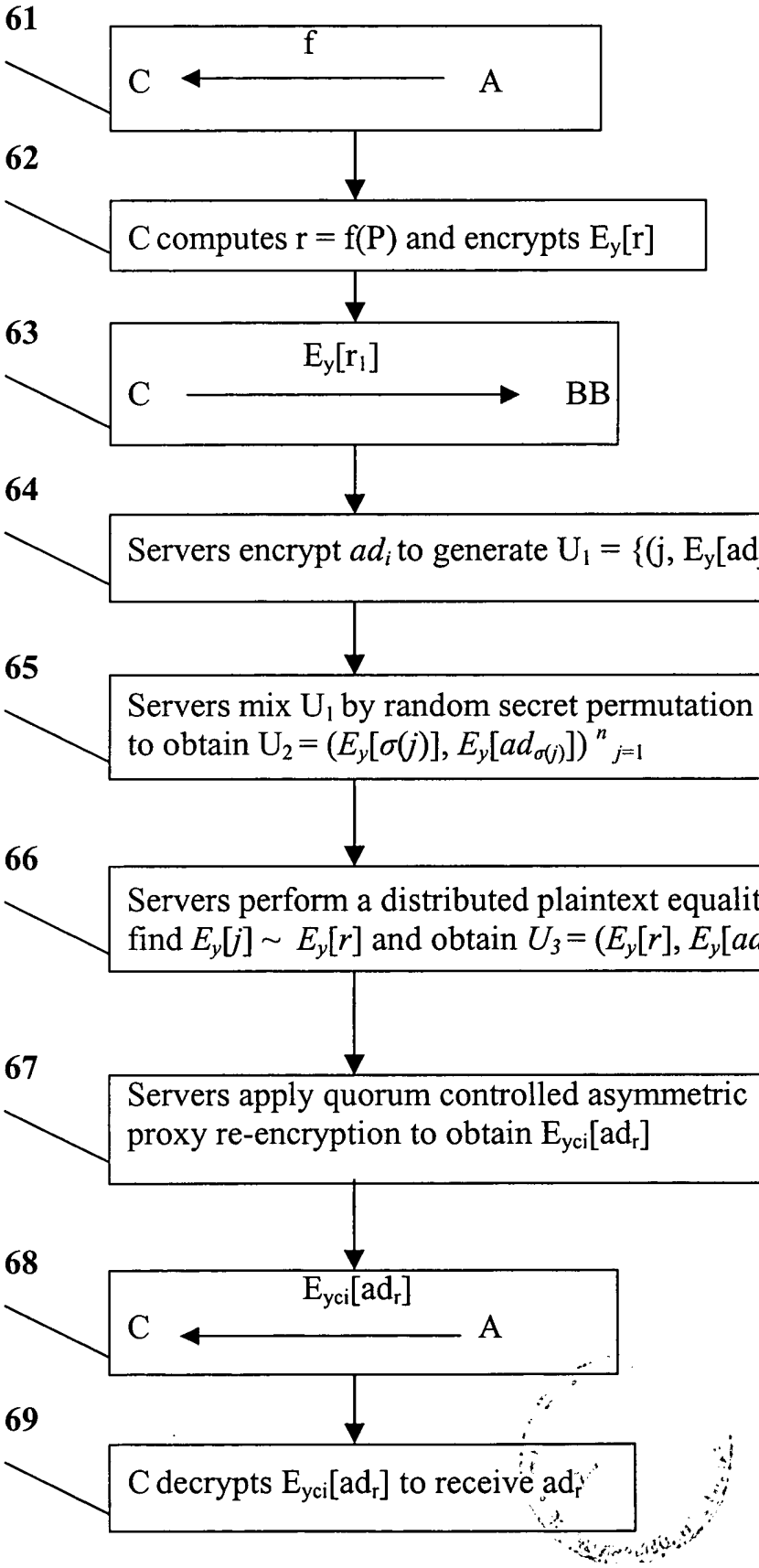
61
f
C
A
62
C computes r = f(P) and encrypts $E_y[r]$
63
$E_y[r_1]$
C
BB
64
Servers encrypt ad_i to generate $U_1 = \{(j, E_y[ad_j])\}^n_{j=1}$
65
Servers mix U_1 by random secret permutation σ to obtain $U_2 = (E_y[\sigma(j)], E_y[ad_{\sigma(j)}])^n_{j=1}$
66
Servers perform a distributed plaintext equality test to find $E_y[j] \sim E_y[r]$ and obtain $U_3 = (E_y[r], E_y[ad_r])$
67
Servers apply quorum controlled asymmetric proxy re-encryption to obtain $E_{yci}[ad_r]$
68
$E_{yci}[ad_r]$
C
A
69
C decrypts $E_{yci}[ad_r]$ to receive ad_r

FIG. 6

2031066-4

D0000000000